0/30 Questions Answered

Time Remaining
1 hr 59 mins

Midterm - Only start when ready -- you only have one chance

Q1 Introduction

10 Points

- The exam auto-submits when the time ends, so please watch the clock. The timer does not stop even if you hit submit (as you can return to the exam).
- The midterm exam is open book, open notes, open VM, and open Internet. However, it must be performed individually -- you may not collaborate or discuss the exam with anyone until the exam grade is released. Please see the definitions of cheating and unauthorized collaboration in the Student Code of Conduct. Usage of ChatGPT or any other AI content generation tools would be considered plagiarism. Turnitin and other plagiarism checkers will be used.
- Always give the best answer. Points deducted when the best answer is not given.
- On areas of the exam where it specifies to show work or explain or where there is a large text box, you must show work/explain for credit. Points will be deducted for answers that are not the best answer or not clear.
- If you encounter a technical error, please email to Professor Mak the answers within five minutes of the end of the exam.

Q1.1 Quantitive Risk Analysis

10 Points

ACME Corporation recently perform a risk assessment and identified several risks.

- Risk 1: The server farm has a 40% chance of failing each year due to hardware malfunction. The replacement cost for the server, including labor and downtime losses, is estimated at $50,000 per incident.
- Risk 2: There's also a risk of a security breach, 50% probability every 24 months, which would leak sensitive client data and it is estimated that it would be $400,000 to secure the breach and repair the PR damage.

For Risk 1:

a. [1 pt] What is the ARO?

b. [1 pt] What is the SLE?

c. [1 pt] What is the ALE?

For Risk 2:

d. [1 pt] What is the ARO?

e. [1 pt] What is the SLE?

f. [1 pt] What is the ALE?

g. [4 pt] ACME is considering implementing a vulnerability management system to mitigate Risk 2. The system would have an initial cost of $200,000 and will require one full-time engineer to manage it (annual salary + benefits of $200,000/year). Given your calculations for Risk 2, would this be a good investment? Provide your rationale with clear supporting calculations. Explain why or why not.

Q2 Reconnaissance
12 Points

A security engineer is tasked with scanning a remote server within a critical infrastructure network.

Q2.1
4 Points

The security engineer performs the following nmap scan:

```
nmap -sS -p 443 192.168.1.10
```

The scan result indicates that port 443 is closed. Explain how nmap was able to determine that. Please give specific protocol level header information on what was sent and received.

Q2.2
4 Points

Suppose the engineer now performs this scan:

```
nmap -sU -p 443 192.168.1.10
```

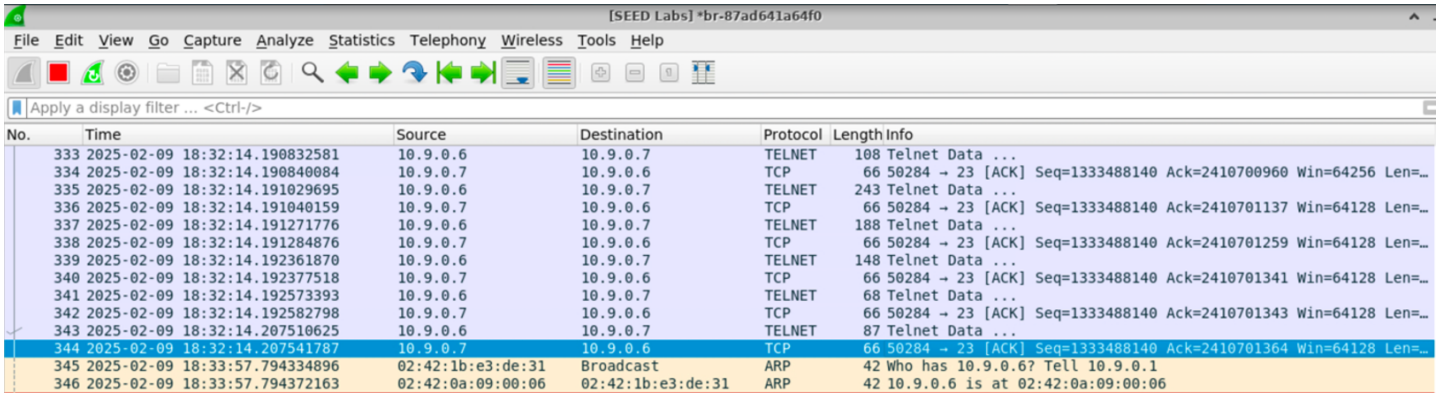
The result says “open|filtered”. Explain what led nmap to determine this. Please give specific protocol level header information on what was sent and received.

Q2.3
4 Points

Suppose the engineer is now analyzing the firewall logs and notices repeated TCP SYN packets to port 445, but no connections. What could this indicate? Explain in detail.

Q3 TCP Attacks

16 Points



The screenshot above shows a telnet connection between Alice and Bob. Suppose Trudy, the attacker, wants to perform a TCP RST attack to break the connection. She wants to attack the client (Alice's) side of the connection. Please fill out the parameters for her code below to successful do that.

```
1  #!/usr/bin/env python3
2  from scapy.all import *
3  ip = IP(src="(A)", dst="(B)")
4  tcp = TCP(sport=(C), dport=(D), flags="(E)", seq=(F), ack=(G))
5  pkt = (H)
6  ls(pkt)
7  send(pkt, verbose=0)
```

Q3.1 Value for (A) - src

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.2 Value for (B) - dst

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.3 Value for (C) - sport

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.4 Value for (D) - dport

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.5 Value for (E) - flags

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.6 Value for (F) - seq

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.7 Value for (G) - ack

2 Points

10.9.0.1

10.9.0.6

10.9.0.7

23

50284

1333488140

2410701364

R

RA

RST

S

SA

Parameter not needed

Q3.8 Value for (H) - pkt

2 Points

Q4 Session Hijacking

14 Points

Suppose Trudy is trying to hijack a telnet session between Alice and Bob, with Alice being the client and Bob being the server.

a. [4 pts] Explain how Trudy can inject malicious commands into the telnet session. Include details about sequence numbers.

b. [6 pts] Explain if it would be useful to Trudy if she blocked communications from Alice. What is the benefit? Describe one way that Trudy can do that.

c. [4 pts] Suppose Trudy is trying to hijack the telnet session, however, she cannot see the traffic on the network and can only blindly inject traffic. Explain how many times she can guess before being locked out of the system, presuming there is no IDS/IPS to stop Trudy.

Q5 RSA
12 Points

Perform RSA key generation. Suppose **p = 53** and **n = 2279**.

Q5.1 What would be the value of q?
2 Points

Q5.2 What would be the value of ϕ?
1 Point

Q5.3 Which are the following are possible values of e? (Choose all that are correct, no partial credit)

3 Points

- [ ] 2
- [ ] 3
- [ ] 5
- [ ] 7
- [ ] 9
- [ ] 11
- [ ] 13
- [ ] 15
- [ ] 17
- [ ] 19
- [ ] 21
- [ ] 22

Q5.4 Suppose e is 23. Find d.

3 Points

Hint: One possible values of *d* is between 80 and 120.

Q5.5 Using e=23, encrypt m=100

3 Points

Q6 Diffie-Hellman
10 Points

Perform Diffie-Hellman shared key generation with **g = 7**, **n = 29**, Alice selects **a = 5** as her secret, and Bob selects **b = 6** as his secret.

Q6.1 calculate Alice's public key A
3 Points

Q6.2 calculate Bob's public key B
3 Points

Q6.3 Calculate the shared key K
4 Points

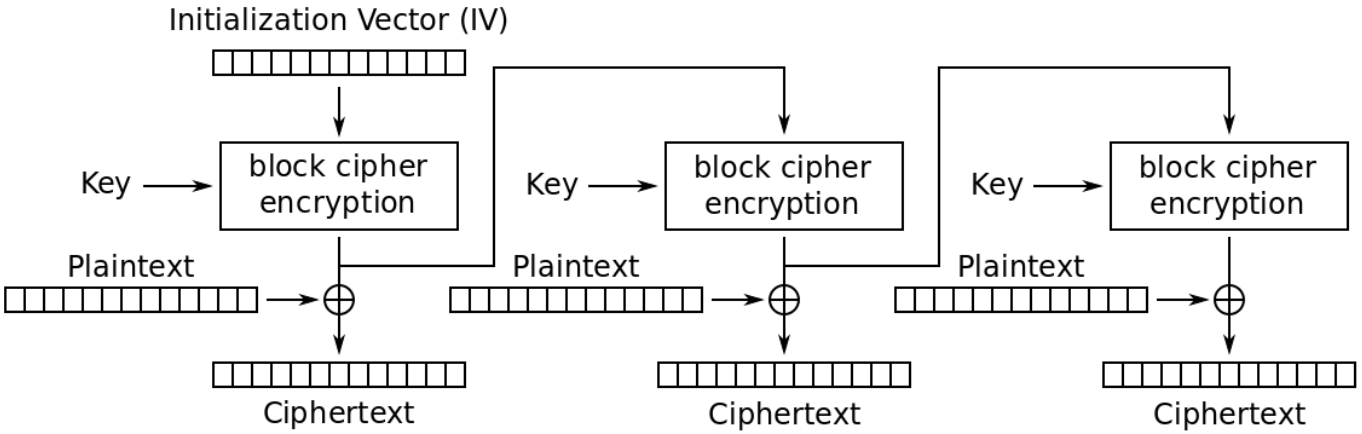
Q7 Block Cipher Mode of Operations

6 Points

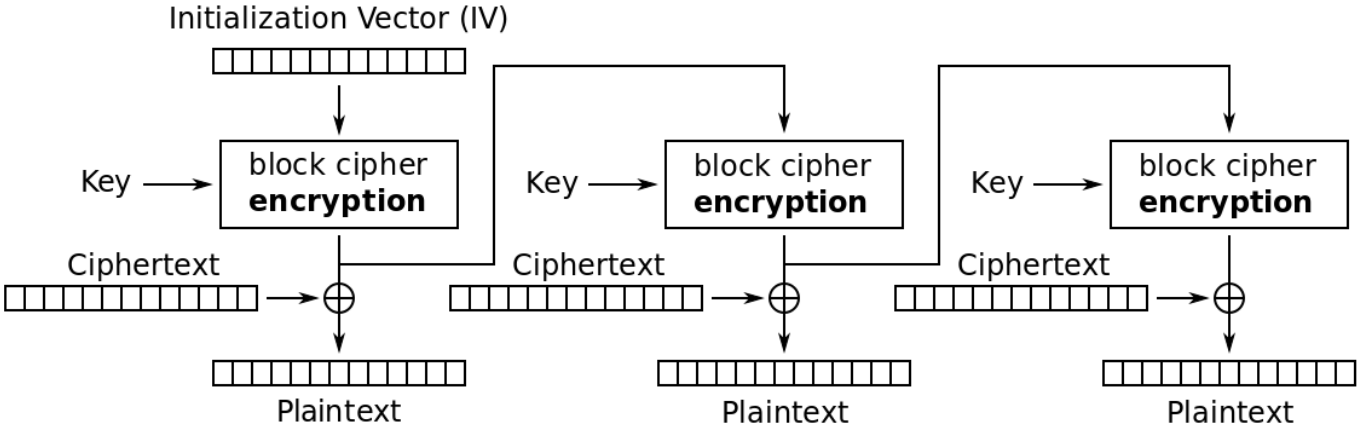
Use the following input/output table (encryption algorithm) for this problem.

Input	Output
000	101
001	011
010	111
011	001
110	000
100	110
101	100
111	010

The following diagram shows Output Feedback Mode (OFB), a similar mode of operation to CBC. **Note that the bottom diagram, which shows decryption, actually uses encryption.**



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Q7.1 Decrypt Ciphertext 010010010010 using OFB and IV=001.

6 Points

Note: Question specifies to **decrypt**.

Q8 Miscellaneous
20 Points

Q8.1 Vigenère
4 Points

Using the standard Vigenère table, encrypt:

`Cyberecurity`

Using the key:

`network`

What is the cipher text?

Q8.2
2 Points

Diffusion in cryptography means changing one character in the key will affect many parts of the ciphertext.

- True
- False

Q8.3
2 Points

AES uses a function for it's substitution table because it would require too much memory to store it as a table.

- True
- False

Q8.4
2 Points

The initialization vector must be kept secret at all costs.

- True
- False

Q8.5
2 Points

CBC is no longer used in encryption because when given two identical blocks of data, it returns the same block of data.

- True
- False

Q8.6
2 Points

RSA Key Creation: What value is impossible in the following:

p = 5

q = 17

n = 85

Φ = 10

Q8.7
2 Points

Which of the following is true about a one-time pad cipher when the key is as long as the message, truly random, and never reused?

It can be broken using frequency analysis.

It is as vulnerable as a Vigenère cipher with a short key.

It is theoretically unbreakable without the key.

It can be cracked if some of the plaintext is known, allowing the attacker to deduce the rest of the key.

Q8.8 tcpdump

4 Points

What is the `tcpdump` option to prevent the tool from **converting packets** and DNS resolution.

Submit & View Submission >